

Installing ssh 1.2.27

ITOS Edition

\$Date: 2006/03/21 16:07:24 \$

Copyright 1999-2006, United States Government as represented by the Administrator of the National Aeronautics and Space Administration. No copyright is claimed in the United States under Title 17, U.S. Code.

This software and documentation are controlled exports and may only be released to U.S. Citizens and appropriate Permanent Residents in the United States. If you have any questions with respect to this constraint contact the GSFC center export administrator, <Thomas.R.Weisz@nasa.gov>.

This product contains software from the Integrated Test and Operations System (ITOS), a satellite ground data system developed at the Goddard Space Flight Center in Greenbelt MD. See <<http://itos.gsfc.nasa.gov/>> or e-mail <itos@itos.gsfc.nasa.gov> for additional information.

You may use this software for any purpose provided you agree to the following terms and conditions:

1. Redistributions of source code must retain the above copyright notice and this list of conditions.
2. Redistributions in binary form must reproduce the above copyright notice and this list of conditions in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product contains software from the Integrated Test and Operations System (ITOS), a satellite ground data system developed at the Goddard Space Flight Center in Greenbelt MD.

This software is provided ‘‘as is’’ without any warranty of any kind, either express, implied, or statutory, including, but not limited to, any warranty that the software will conform to specification, any implied warranties of merchantability, fitness for a particular purpose, and freedom from infringement and any warranty that the documentation will conform to their program or will be error free.

In no event shall NASA be liable for any damages, including, but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this software, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained by persons or property or otherwise, and whether or not loss was sustained from or arose out of the results of, or use of, their software or services provided hereunder.

Installing and Configuring ssh 1.2.27

This describes how we install and configure ssh on ITOS computers. These instructions apply to Linux only.

Obtaining ssh

Get 'ssh-1.2.27.tar.gz' and 'rsaref2.tgz' from a trusted site.

About our installation

In the following, \$DISTDIR is the directory containing the distribution tar files and \$WORKDIR is the directory where you're gonna build ssh.

Installing ssh

On Solaris and FreeBSD

```
# cd $WORKDIR
# tar zxvf $DISTDIR/ssh-1.2.26.tar.gz
# cd ssh-1.2.26
# tar zxvf $DISTDIR/rsaref2.tgz
# cp /usr/local/lib/libwrap.a .
# cp /usr/local/include/tcpd.h .
# ./configure --with-rsaref --with-libwrap \
--with-rsh=/usr/bin/insecure/rsh
# make
# make install
```

On Linux

```
# cd /usr/bin
# mkdir insecure
# cp rsh insecure
# cp rcp insecure
# cp rlogin insecure
# cd $WORKDIR
# tar zxvf $DISTDIR/ssh-1.2.27.tar.gz
# cd ssh-1.2.27
# tar zxvf $DISTDIR/rsaref2.tar.gz
# cp /usr/lib/libwrap.a .
# cp /usr/include/tcpd.h .
# ./configure --with-rsaref --with-libwrap \
--with-rsh=/usr/bin/insecure/rsh
# make
# make install
```

This created `/etc/ssh_host_key`; when restoring a dump to a different system be sure to delete `/etc/ssh_host_key` and re-create it via

```
# ssh-keygen -b 1024 -f /etc/ssh_host_key -N ''
```

Continuing the installation:

```
# cp /usr/local/sbin/sshd1 /usr/sbin
# ln -s /usr/sbin/sshd1 /usr/sbin/sshd
# cd /usr/bin
# mkdir insecure
# mv rsh rlogin rcp insecure
```

We also like to configure CDE to work with *ssh*. This involves editing `/usr/dt/bin/Xsession`:

```
# cd /usr/dt/bin
/usr/dt/bin
# mv Xsession Xsession-real
# cat > Xsession
#!/bin/ksh
if [ -x /usr/local/bin/ssh-agent -a -d ~/.ssh ]; then
    /usr/local/bin/ssh-agent /usr/dt/bin/Xsession-real
else
    . /usr/dt/bin/Xsession-real
fi
(D)
# chmod a+x Xsession
# chmod a-w Xsession
#
```

On FreeBSD ...

Edit `/etc/rc.local`. At the bottom of the file, add the line:

```
[ -x /usr/sbin/sshd ] && /usr/sbin/sshd && echo "sshd"
```

On Linux ...

Edit `/etc/rc.d/rc.sysinit`. At the bottom of the file, add the lines:

```
# Start ssh daemon
[ -x /usr/sbin/sshd ] && /usr/sbin/sshd && echo "sshd"
```

If necessary add a logical link for users shell.

```
ln -s /bin/bash /usr/local/bin/bash
ln -s /bin/bash2 /usr/local/bin/bash
```

`/etc/hosts.allow`

The following applies to all operating systems ...

We built ssh `--with-libwrap` which means that ssh will look at `/etc/hosts.deny` and `/etc/hosts.allow` as its first line of defense, and uses the daemon names *sshd* and

sshd-X11. To grant ssh access to machines, edit `/etc/hosts.allow` and add a line like:

```
sshd sshd-X11: .nasa.gov trusted.machine.com trustme.too.com
```

(Of course, don't literally add this line).